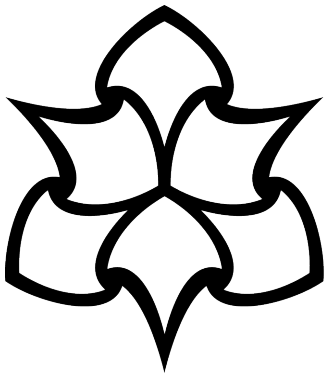

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 16, 2020, accepted April 27, 2020, date of publication May 6, 2020, date of current version May 29, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.2992820*

# Providing End-to-End Security Using Quantum Walks in IoT Networks

**AHMED A. ABD EL-LATIF[1,2], (Member, IEEE), BASSEM ABD-EL-ATTY[2], SALVADOR E. VENEGAS-ANDRACA[3], HAITHAM ELWAHSH[4], MD. JALIL PIRAN[5], (Member, IEEE), ALI KASHIF BASHIR[6], OH-YOUNG SONG[7], AND WOJCIECH MAZURCZYK[8]**

[1]Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
[2]Center of Excellence in Cybersecurity, Quantum Information Processing, and Artificial Intelligence, Menoufia University, Shebin El-Koom 32511, Egypt
[3]Tecnologico de Monterrey, Escuela de Ingenieria y Ciencias, Monterrey 64849, Mexico
[4]Computer Science Department, Faculty of Computers and Information, Kafrelsheikh University, Kafrelsheikh 33516, Egypt
[5]Computer Engineering Department, Sejong University, Seoul 05006, South Korea
[6]Department of Computing and Mathematics, Manchester Metropolitan University, Manchester M15 6BH, U.K.
[7]Software Department, Sejong University, Seoul 05006, South Korea
[8]Institute of Computer Science, Warsaw University of Technology, 00-665 Warsaw, Poland

Corresponding authors: Ahmed A. Abd El-Latif (a.rahiem@gmail.com) and Oh-young Song (oysong@sejong.edu)

The work of Ahmed A. Abd El-Latif was supported by the Menoufia University, Egypt. This research was supported in part by MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2020-2016-0-00312) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation), in part by the Tecnologico de Monterrey, Escuela de Ingenieria y Ciencias and CONACyT under SNI 41594, in part by the Fronteras de la Ciencia under Project 1007, and in part by the National Centre for Research and Development, Poland under Gospostrateg Programme framework and more specifically 5G@PL Project en-titled Deployment of 5G network in Polish Market under Grant Gospostrateg 1/383021/19/NCBR/2018.

**ABSTRACT** Internet of Things acts an essential role in our everyday lives and it definitely has the potential to grow on the importance and revolutionize our future. However, the present communication technologies have several security related issues which is required to provide secure end to end connectivity among services. Moreover, due to recent, rapid growth of quantum technologies, most common security mechanisms considered secure today may be soon imperilled. Thus, the modern security mechanisms during their construction also require the power of quantum technologies to resist various potential attacks from quantum computers. Because of its characteristics, quantum walks (QW) is considered as a universal quantum computation paradigm that can be accepted as an excellent key generator. In this regard, in this paper a new lightweight image encryption scheme based on QW for secure data transfer in the internet of things platforms and wireless networking with edge computing is proposed. The introduced approach utilises the power of nonlinear dynamic behaviour of QW to construct permutation boxes and generates pseudo-random numbers for encrypting the plain image after dividing it into blocks. The results of the conducted simulation and numerical analyses confirm that the presented encryption algorithm is effective. The encrypted images have randomness properties, no useful data about the ciphered image can be obtained via analysing the correlation of adjacent pixels. Moreover, the entropy value is close to 8, the number of the pixel change rate is greater than 99.61%, and there is high sensitivity of the key parameters with large key space to resist various attacks.

**INDEX TERMS** Quantum walks, lightweight cipher, data transfer in IoT, image encryption, edge computing, wireless communication.

## I. INTRODUCTION

The Internet of Things (IoT) has heightened an integral part of the future of communication systems [1], [2]. It promises vast interconnections of ''things'' including everything, everyone, everywhere, every time and every network. Within this concept, smart nodes comprising devices, sensors, services, applications, etc. will be able to seamlessly interact and communicate in real time. In addition, to interconnecting devices, IoT will usher in web-enabled exchange of data which will enhance service delivery. Moreover, IoT will also provide a platform to integrate the physical world with the virtual one. From this perspective, considering the envisioned importance of IoT, data security should be treated as the backbone of data transfer in IoT environments.

The associate editor coordinating the review of this manuscript and approving it for publication was Jun Wu.

The protection of data transfer from unauthorized access in IoT systems becomes a pressing issue and is increasingly investigated by experts and researchers [3]–[8]. Techniques for protecting digital information can be roughly classified into two groups. The first type is data encryption and the other is data hiding [9]–[14]. In this context, data encryption refers to transformations of the original data from an intelligible form into an unidentifiable one [15]. Digital images are one of the common data representation patterns which are extensively used in numerous applications.

Recently, various image encryption mechanisms have been proposed [16]–[22] and most of them are based on mathematical models such as chaotic systems. Nevertheless, because of the periodicity chaos property, most chaotic models are unstable [23]. Consequently, most chaos-based image encryption mechanisms are susceptible to attacks [24].

Quantum computers have shown promise for operations unrivalled by the best-known digital resources due to quantum phenomena like quantum superposition and quantum entanglement [25], [26]. Considering its roots in quantum mechanics, which relies on the linear algebraic formulations as well as applications in computing, device fabrication, etc., quantum computing is a promising concept for a wide range of disciplines including physics, mathematics, computer science, and engineering. This multidisciplinary undertaking is already shaping innovations and technologies in information theory, communication, cryptography, image processing and electronics, among many other fields. In all these areas, quantum computation has been deployed to improve the existing non-quantum algorithms and technologies. Moreover, the reinvigorated efforts to realize physically scalable quantum hardware have reinforced the belief that when (not if) quantum computers are fully completed they will be capable of solving many computing issues considered intractable via available (digital) resources.

However, in the wrong hands, the immense capabilities of quantum computing can be misused. In this manner, they pose unprecedented threat to today's information security mechanisms. These threats range from exploiting the vulnerabilities inherent to cybersecurity frameworks to issues or gaps arising from the transition or widespread prevalence of quantum computing hardware. Therefore, modern cryptographic mechanisms require incorporating quantum technology to withstand possible attacks from quantum devices in the near future [27]. In this regard, risks related to data transfer in IoT platforms would be greatly mitigated or eliminated via advanced cryptographic mechanisms based on quantum technologies.

Quantum walks (QW) is considered as a universal quantum computational model [28]–[30], that can be accepted as a good key generator because of its inherent nonlinear chaotic dynamical behaviour [31]–[40]. QW similarly to chaos has chaotic behaviour and high sensitivity to initial conditions. Moreover, QW possesses advantages like non-periodicity, stability and theoretically infinite keyspace to withstand various attacks. In this manner, El-Latif et al [32] presented a novel idea for cascading quantum inspired QWs with chaotic systems and present its cryptographic application. Also, Yang et al [33] designed an image encryption mechanism using two-walker QW. Then, Yang et al [34] presented a new scheme for constructing hash function using controlled two-walker QW and introduced its application to image encryption, Next, El-Latif et al [35] constructed a substitution-box mechanism based on two-walker QW and presented its application in image steganography. However, the implementation of two-walker QW requires more physical resources than the realization of one-walker QW [41], that is why consequently Abd-El-Atty et al [36] designed a quantum encryption approach based on controlled one-walker QW. Finally, El-Latif et al [37] presented an image encryption approach using controlled alternate QW for privacy preserving medical images in IoT systems.

The key contribution of this paper is a proposal of a new lightweight image cipher scheme using one-walker QWs on a circle for secure data transfers in IoT platforms. The aspects of the new scheme is based on lightweight structure in confusion and diffusion processes. It utilises the power of nonlinear dynamics of QW to construct P-boxes for confusion and to generate PRNGs in diffusion. At first, the original object is divided into blocks, and then each block is divided into two subblocks: right subblock and left subblock. Each subblock before recombination with each other is permutated and substituted with its own P-box and PRNG sequence that originates from the probability distribution of running QW. The ciphered blocks are combined together and then XORed with another PRNG sequence to construct the ciphered image. Several enclosed simulation and numerical analyses are conducted based on differential and statistical analyses, which affirm the effectiveness of the proposed cipher. The resulted cipherimages have randomness properties, no useful data about the ciphered image can be obtained via analysing the correlation of adjacent pixels. Moreover, the entropy value is close to the optimal value, NPCR test rate is greater than 99.61%, and there is high key sensitivity in the parameters of the keys with large key space to resist various cyberanalysis.

The key contributions of our paper can be summarized as:

- Propose a new lightweight cipher scheme using QWs.
- The presented mechanism is utilised for securing data transfers in IoT platforms.
- The aspects of the presented cryptosystem are based on a lightweight structure in confusion and diffusion processes.
- The presented mechanism utilises the power of nonlinear dynamics of QW to construct P-boxes for confusion and to generate PRNGs for diffusion stage.

The outline of this work is as follows: the preliminary knowledge for QW is presented in Section II, while the proposed framework for secure data transfers in IoT environments is presented in Section III. Next, Section IV presents our lightweight image encryption approach, while the numerical analyses and simulation outcomes are given in Section V. Finally, Section VI concludes our work.

## II. PRELIMINARY KNOWLEDGE

There are two models of quantum walks: continuous-time quantum walk and discrete-time quantum walk (QW) [28]. In this paper, we focus only on QW, which is widely used in designing modern cryptographic applications [31]–[40]. The elementary components of running one-walker QW acting on a circle have two quantum systems: a particle $|\psi\rangle_p$ known as a walker living in a p-dimensional Hilbert space $H_p$ and a 2-dimensional quantum system $|\psi\rangle_c = \cos\ \alpha|0\rangle + \sin\ \alpha|1\rangle$ known as a coin living in Hilbert space $H_c$. The total Hilbert space of the QW is $H = H_p \otimes H_c$. In every step $r$ of running QW on a circle, the unitary transformation $\hat{R}$ is executed on the whole quantum system $|Q\rangle$. The unitary transformation $\hat{R}$ can be expressed as in Eq. (1).

$$\hat{R} = \hat{F}(\hat{I} \otimes \hat{U}) \tag{1}$$

here $\hat{F}$ points to the shift operator and can be stated for running QW on a circle with $T$ vertices as in (2).

$$\hat{F} = \sum_{i=0}^{T-1} (|(i+1)\ \bmod T, 0\rangle\langle i, 0| + |(i-1)\ \bmod T, 0\rangle\langle i, 1|) \tag{2}$$

Also, operator $\hat{U}$ points to a coin operator $2\times 2$ and in general case can be stated as in (3)

$$\hat{U} = \begin{pmatrix} \cos\ \beta & \sin\ \beta \\ \sin\ \beta & -\cos\ \beta \end{pmatrix} \tag{3}$$

After $r$ steps, the final state $|Q\rangle_r$ can be stated as in (4)

$$|Q\rangle_r = \left(\hat{R}\right)^r |Q\rangle_0 \tag{4}$$

and after $r$ steps, the probability of locating the particle at location $i$ can be expressed as in (5)

$$P(i, r) = \left|\langle i,0| \left(\hat{R}\right)^r |Q\rangle_0\right|^2 + \left|\langle i,1| \left(\hat{R}\right)^r |Q\rangle_0\right|^2 \tag{5}$$

## III. PROPOSED FRAMEWORK FOR SECURE DATA TRANSFERS IN IoT PLATFORMS

IoT covers a huge amount of information, which refers to a rapidly growing network of objects or connected devices that are able to collect data using sensors and share this data via networks, e.g. Internet [42]. The immense potential of IoT has seen its use in many areas, including smart cities, smart homes, smart cars, telemedicine, etc. [2], [43]. These vastly interconnected devices need to gather real-time information and connect them to other cloud resources to collect, store, and analyse different data streams [44]. All these processes have an impact on privacy and security of sensitive information. For example, the confidential health records of patients, geotagging people's location using wearable devices [45], [46] need to be safely guarded against the ever-increasing sophistication of criminals. In smart cities, IoT can include important data to control and monitor installations as well as private information of inhabitants of the city [43], [47]. Securing such sensitive information from malicious attacks becomes currently the most pressing aspect of IoT [48]. Currently, the security fabric of the Internet is not sufficient due to the lack of appropriate security and integrity, susceptibility to systems and physical access, etc. Apart from these issues, since most devices communicate in a wireless manner thus IoT applications should work perfectly in the presence of security challenges. To deal with these security risks a system that is capable to identify and diagnose attacks in necessary. Due to the low-capacity of IoT devices, operations need to be performed using lightweight security mechanisms that can deal with various attacks [49]. With subsisting centralized security solutions which require heavyweight computing and large memory, finding solutions for lightweight security for IoT scenarios is a challenge with many open research areas. That is why, in this paper we provide a new lightweight cipher using one-walker QW for secure data transfers in IoT systems. The presented framework is based on QW to deal with various attacks and resist the feasible threats from quantum computers in the coming future. The outline of the presented framework is provided in Fig. 1.

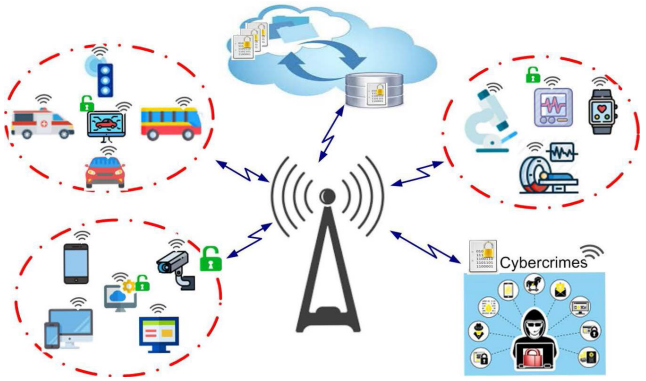


**FIGURE 1.** Propounded framework for secure data transfers in IoT.

## IV. PROPOSED LIGHTWEIGHT IMAGE ENCRYPTION MECHANISM

In this section, we introduce a new lightweight image encryption mechanism using one-walker QW. The presented solution utilises the capabilities of nonlinear dynamics of QWs to generate PRNG sequences and construct P-boxes. At first, the original image is divided into blocks each of size $16 \times 16$, and then each block is divided into two subblocks: right subblock (RB) and left subblock (LB). Each subblock before recombination is permutated and substituted with its own P-box and PRNG that originates from the probability distribution of acting one-walker QW on a circle. The ciphered blocks are combined together and then XORed with another PRNG sequence to construct the cipher image. The suggested lightweight image encryption algorithm is outlined in Fig. 2 and the encryption and decryption procedures are presented in Algorithms 1 and 2, respectively.

## V. SIMULATION RESULTS

To validate the presented image encryption mechanism, we utilised a laptop with 6-GB RAM and Intel *Core*$^{TM}$

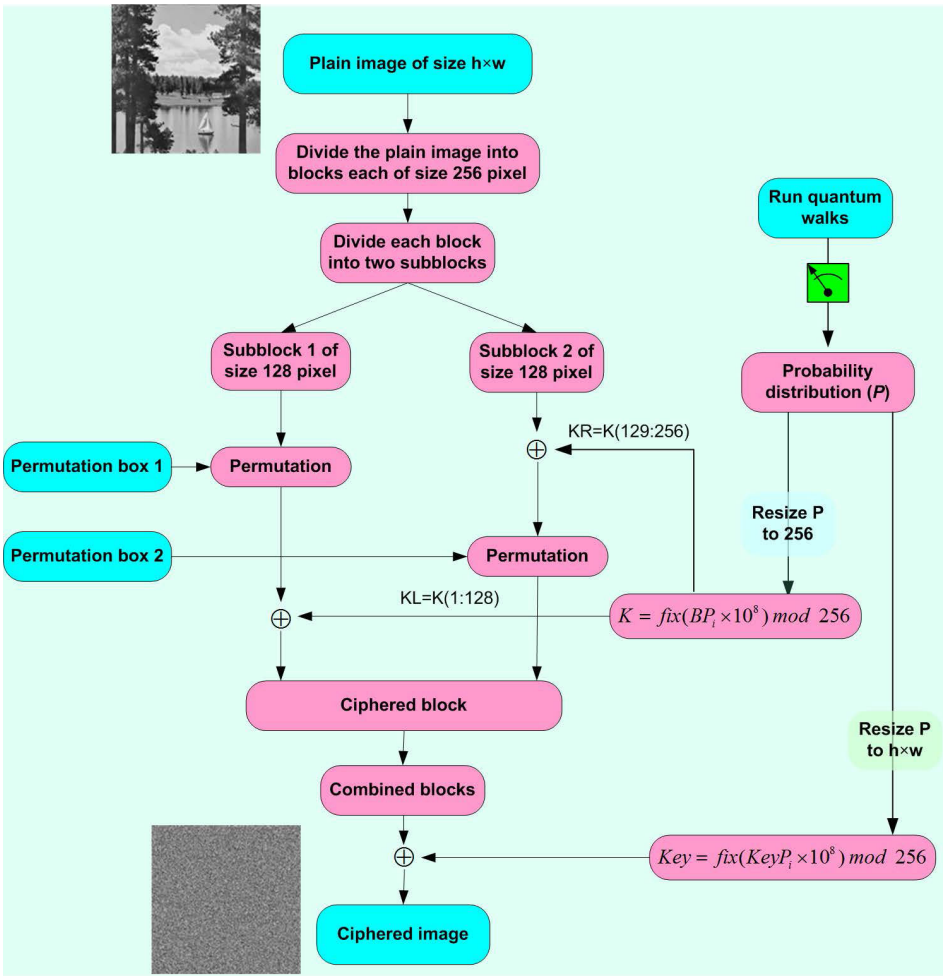


**FIGURE 2.** The encryption procedure where the permutation and substitution procedures are based only on QWs and the procedure of constructing permutation boxes is provided in Fig. 3.

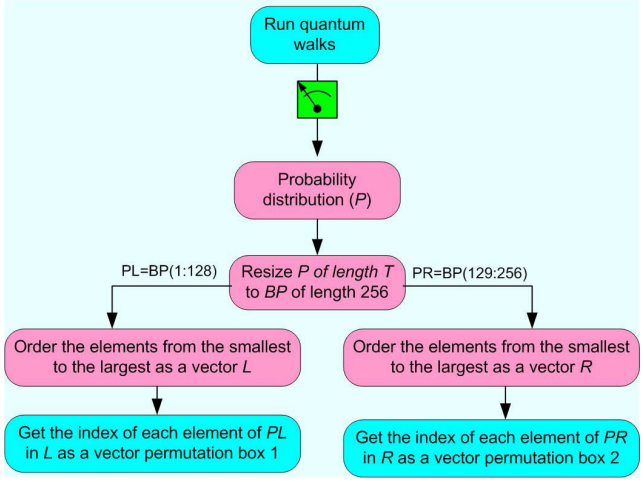


**FIGURE 3.** The procedure of constructing permutation boxes which are used to permutate subblocks.

i5 CPU 2.50-GHz with preinstalled MATLAB R2016b. The used dataset of images (Sailboat, Baboon, Houses, and Aerial) consists of greyscale images each of size 512 × 512 (see Fig. 4), while the initial values utilized for operating one-walker QW on a circle are ($T = 241$, $r = 265$, $\alpha = 0$, $\beta = \pi/3$).

### A. RANDOMNESS ANALYSIS

NIST SP 800-22 tests are applied to investigate the randomness behavior of the produced key (key sequence) and the constructed cipher image (CIm) and they consist of 15 tests that are applied on a $10^6$ bit sequence. The NIST results of key sequence (Key) and the cipher Sailboat image (Enc-Sailboat) are stated in Table 1, which passed all randomness tests. Therefore, the proposed encryption mechanism can be reliably used on modern cryptographic mechanisms.

### B. CORRELATION ANALYSIS

One of the most important tools to evaluate an ciphered image is its correlation coefficient of adjacent pixels $Cor_{pc}$. The typical images have $Cor_{pc}$ close to 1 in each direction while in ciphered images with a well-designed encryption mechanism it should be near 0. To measure $Cor_{pc}$ of the plain and ciphered images, we picked at random $10^4$ pairs

**Algorithm 1** Encryption Procedure

**Input**: Plain image (PIm) and key parameters for running one-walker QW($T$, $r$, $\alpha$, $\beta$)
**Output**: Cipher-image (CIm)

$P \leftarrow QW(T,\ r,\ \alpha,\ \beta)$ // Run quantum walks on a circle of odd T vertices for r steps, where the initial walker is $H_c = \cos\ \alpha|0\rangle + \sin\ \alpha|1\rangle$, *and* $\beta$ *is used to construct the operator* $\hat{U}$ *where* $\alpha, \beta \in [0, \pi/2]$
$[h\ w] \leftarrow size(PIm)$// Gets the size of the plain image
// Construct two permutation boxes each of length 128 (see Fig.3)
$BP \leftarrow Resize(P, [1256])$// Resize the probability distribution P of length T to BP of length 256
// For constructing permutation box1
$PL \leftarrow BP(1:128)$
$L \leftarrow order(PL)$// Arrange in ascending order the elements of sequence PL
$P-box1 \leftarrow index(PLinL)$// For each element in sequence PL, gets its index in sequence L
// For constructing permutation box2
$PR \leftarrow BP(129:256)$
$R \leftarrow order(PR)$
$P-box2 \leftarrow index(PRinR)$
$K \leftarrow fix(BP \times 10^8)\ \bmod 256$ // Converting BP sequence into integer values
$KeyP \leftarrow Resize(P, [1\ \ h \times w])$ // Resize P of length T to h×w
$Key \leftarrow fix(KeyP \times 10^8)\ \bmod 256$
$Key \leftarrow reshape(Key, h, w)$ // Transform the key sequence into matrix
$Blocks[\ ] \leftarrow dividePImintoblockseachofsize16 \times 16$
**for** *each* $Block \leftarrow Blocks[\ ]$ **do**
  $block \leftarrow reshape(block, 1, 256)$
  $LB \leftarrow block(1:128)$ // Subblock1
  $RB \leftarrow block(129:256)$ // Subblock2
  $RB1 \leftarrow bitxor(RB, K(129:256))$ // Substitute subblock2
  **for** $i \leftarrow 1$ *to* 128 **do**
    $LB1(i) \leftarrow LB(P-box1(i))$ // Permute subblock1
  **for** $i \leftarrow 1$ *to* 128 **do**
    $RB2(i) \leftarrow RB1(P-box2(i))$ // Permute subblock2
  $LB2 \leftarrow bitxor(LB1, K(1:128))$ // Substitute subblock1
  // Combine the cipher subblock1 and subblock2
  $Encblock(1:128) \leftarrow LB2$
  $Encblock(129:256) \leftarrow RB2$
  $Encblock \leftarrow reshape(Encblock, 16, 16)$
  $EncIm \leftarrow combineEncblockintoEncImimage$
$CIm \leftarrow bitxor(EncIm, Key)$ // cipher image

of adjoining pixels. The $Cor_{pc}$ can be calculated via Eq. (6)

$$Cor_{pc} = \frac{\sum_{i=1}^{N}(p_i - \bar{p})(c_i - \bar{c})}{\sqrt{\sum_{i=1}^{N}(p_i - \bar{p})^2 \sum_{i=1}^{N}(c_i - \bar{c})^2}} \tag{6}$$

here $N$ indicates the entire number of adjacent pixel pairs in each direction and $c_i, p_i$ are pointing to the values of adjacent pixels. Table 2 displays the outcomes of $Cor_{pc}$ for ciphered images and as it can be seen they are very close to 0 as well as the original ones. Also, Fig. 5 displays the correlation distribution in each direction for Sailboat image as well as for its ciphered version. From the outcomes stated in Table 2 and the acquaintance displayed in Fig. 5, no useful data can be inferred about the ciphered image by analysing $Cor_{pc}$ values.

### C. NPCR

NPCR ("Number of pixel change rate") is a tool utilized to calculate the influence of varying pixel values in the plain image on the identical ciphered ones, which can be expressed as in (7).

$$NPCR = \frac{\sum_{a;b} D(a,b)}{A} \times 100\%,$$
$$D(a,b) = \begin{cases} 0\ if\ P(a,b) = C(a,b) \\ 1\ if\ P(a,b) \neq C(a,b) \end{cases} \tag{7}$$

**Algorithm 2** Decryption Procedure

**Input**: Cipher-image (CIm) and key parameters for running one-walker QW($T$, $r$, $\alpha$, $\beta$)
**Output**: Decrypted-image (DIm)

$P \leftarrow QW(T,\ r,\ \alpha,\ \beta)$ // Run quantum walks on a circle of odd T vertices for r steps
$[h\ w] \leftarrow size(CIm)$ // Gets the size of the ciphered image
// Construct two permutation boxes each of length 128 (see Fig. 3)
$BP \leftarrow Resize(P, [1\ 256])$ // Resize the probability distribution P of length T to BP of length 256
// For constructing permutation box1
$PL \leftarrow BP(1:128)$
$L \leftarrow order(PL)$
$P-box1 \leftarrow index(PLinL)$
// For constructing permutation box2
$PR \leftarrow BP(129:256)$
$R \leftarrow order(PR)$
$P-box2 \leftarrow index(PRinR)$
$K \leftarrow fix(BP \times 10^8 \mod 256$ // Converting BP sequence into integer values
$KeyP \leftarrow Resize(P, [1\ h \times w])$
$Key \leftarrow fix(KeyP \times 10^8) \mod 256$
$Key \leftarrow reshape(Key, h, w)$// Transform the key sequence into matrix
$DecIm \leftarrow bitxor(CIm, Key)$// bitwise XOR operation
$Blocks[\ ] \leftarrow divideDecImintoblockseachofsize16 \times 16$
**for** *each* $Block \leftarrow Blocks[\ ]$ **do**
  $block \leftarrow reshape(block, 1, 256)$
  $LB \leftarrow block(1:128)$// Subblock1
  $RB \leftarrow block(129:256)$// Subblock2
  **for** $i \leftarrow 1to128$ **do**
    $RB1(P-box2(i)) \leftarrow RB(i)$ // Permute subblock2
  $LB1 \leftarrow bitxor(LB, K(1:128))$ // Substitute subblock1
  $RB2 \leftarrow bitxor(RB1, K(129:256))$ // Substitute subblock2
  **for** $i \leftarrow 1to128$ **do**
    $LB2(P-box1(i)) \leftarrow LB1(i)$ // Permute subblock1
  // Combine the decrypted subblock1 and subblock2
  $Decblock(1:128) \leftarrow LB2$
  $Decblock(129:256) \leftarrow RB2$
  $Decblock \leftarrow reshape(Decblock, 16, 16)$
  $DIm \leftarrow combineDecblockintoDImimage$

here $A$ indicates the whole number of pixels in the image, $C$ and $P$ point to the ciphered and plain images, respectively. The NPCR outcomes for the examined dataset are provided in Table 3, in which we can see that NPCR values are greater than 99.612%. As a result, it can be concluded that the suggested approach is highly sensitive to tiny pixel mutations in the original image.

### D. HISTOGRAM ANALYSIS

Histogram analysis represents the frequency of pixel distribution in an image. A robust encryption approach ought to guarantee the uniform distribution for distinct ciphered images to stand toward statistical attacks. The histograms of the images from the utilized dataset are illustrated in Fig. 6. Note that they are dissimilar from each other. At the same time, the histograms of their corresponding encrypted versions are practically identical. This means that the presented algorithm could resist histogram analyses attack.

### E. GLOBAL ENTROPY ANALYSIS

One of the most important statistical tests to indicate the pixel values distribution for each level in the image is global entropy which can be expressed as follows:

$$E(X) = -\sum_{i=0}^{255} p(x_i) \log_2 (p(x_i)) \tag{8}$$

here $p(x_i)$ refers to the probability of $x_i$. There are $2^8$ possible values for a greyscale image, therefore, in an ideal case entropy should be equal to 8 bits. Hence, to assert the

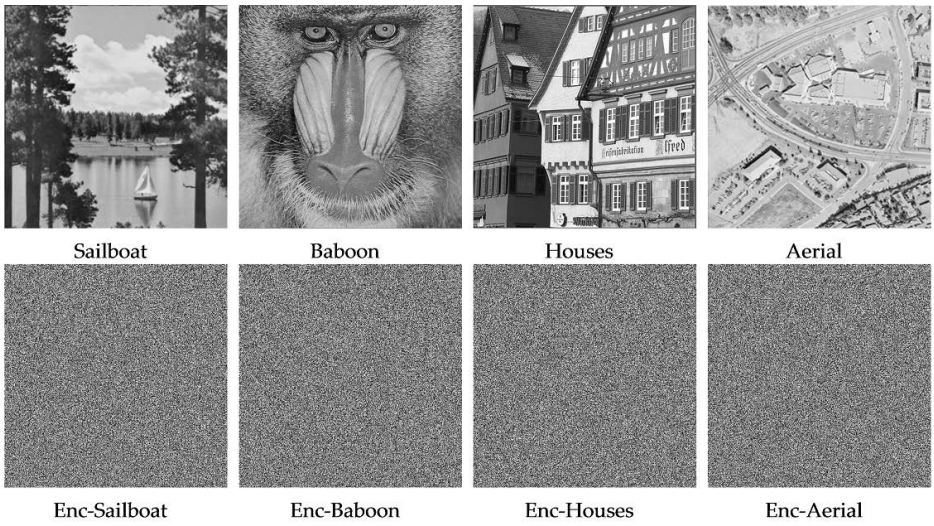


**FIGURE 4.** The first row of images represents the experimental dataset of images each of size 512 × 512, while the second row represents its corresponding ciphered versions.

**TABLE 1.** Outcomes of NIST SP 800-22 tests.

| Name of the test | P-Value | | |
|---|---|---|---|
| | Key | Encrypted Sailboat | Passed |
| Long runs of ones | 0.645169 | 0.822031 | Yes |
| Runs | 0.469972 | 0.675904 | Yes |
| Rank | 0.865578 | 0.466365 | Yes |
| DFT | 0.890517 | 0.970719 | Yes |
| Block-frequency | 0.297495 | 0.996969 | Yes |
| Frequency | 0.469066 | 0.807231 | Yes |
| Universal | 0.154155 | 0.745735 | Yes |
| No overlapping templates | 0.868040 | 0.393861 | Yes |
| Overlapping templates | 0.988637 | 0.857940 | Yes |
| Cumulative sums (reverse) | 0.764505 | 0.673618 | Yes |
| Cumulative sums (forward) | 0.794907 | 0.462727 | Yes |
| Linear complexity | 0.943555 | 0.776374 | Yes |
| Approximate entropy | 0.802852 | 0.238003 | Yes |
| Random excursions variant x=1 | 0.709448 | 0.406777 | Yes |
| Random excursions x=1 | 0.515296 | 0.872236 | Yes |
| Serial test 1 | 0.355836 | 0.833744 | Yes |
| Serial test 2 | 0.157145 | 0.728918 | Yes |

**TABLE 2.** $Cor_{pc}$ values for the utilized experimental dataset.

| image | Direction | | |
|---|---|---|---|
| | Horizontal | Vertical | Diagonal |
| Sailboat | 0.9726 | 0.9762 | 0.9598 |
| Enc-Sailboat | -0.0029 | 0.0001 | -0.0009 |
| Baboon | 0.76030 | 0.8608 | 0.7230 |
| Enc- Baboon | -0.0016 | -0.0012 | 0.0014 |
| Houses | 0.9188 | 0.9047 | 0.8292 |
| Enc- Houses | 0.0004 | 0.0015 | 0.0029 |
| Aerial | 0.8693 | 0.9021 | 0.8130 |
| Enc-Aerial | 0.0016 | -0.0006 | -0.0011 |

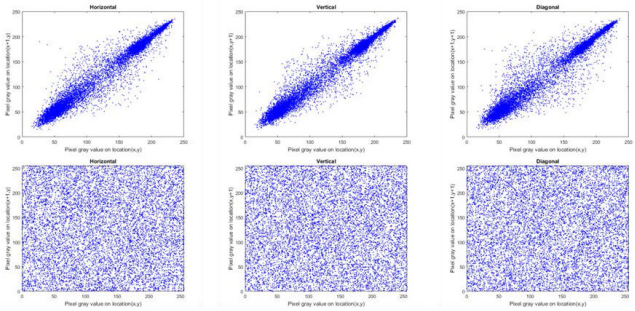

**FIGURE 5.** $Cor_{pc}$ of two neighbouring pixels for Sailboat image, where the first row denotes the plain Sailboat image, and the last row indicates its ciphered version.

**TABLE 3.** NPCR values for the experimental dataset.

| Image | NPCR % |
|---|---|
| Sailboat | 99.61204 |
| Baboon | 99.62501 |
| Houses | 99.61318 |
| Aerial | 99.62082 |

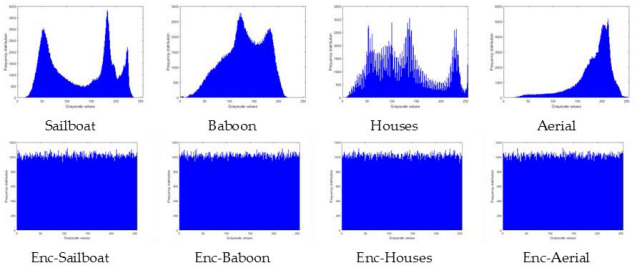


**FIGURE 6.** Histograms of the encrypted and original images from the dataset.

effectiveness of the designed mechanism, the value of entropy for the ciphered image must be as near to 8 as possible. Table 4 shows the outcomes of information entropy for the original images and the corresponding ciphered ones. Note that, all outcomes of information entropy for the ciphered images are extremely close to 8 bits. Thus, the suggested approach is secure under entropy attacks.

**TABLE 4.** Values of information entropy.

| Image | Original | Encrypted |
|---|---|---|
| Sailboat | 7.45696 | 7.99926 |
| Baboon | 7.35788 | 7.99930 |
| Houses | 7.65475 | 7.99925 |
| Aerial | 6.99399 | 7.99924 |

### F. KEY SPACE AND KEY SENSITIVITY ANALYSES

A robust encryption approach should have a sufficient keyspace to withstand brute-force attacks. Our encryption mechanism is based on running one-walker QW on a cycle where the initial values $(T, r, \alpha, \beta)$ are required for operating QW. By considering the calculation precision for digital computers as $10^{-16}$, the total keyspace of the encryption algorithm is $2^{212}$, which is sufficient for any encryption mechanism. Moreover, the key space can be enriched by running controlled one-walker QW on a circle [36].

Key sensitivity is an essential test to ensure the security of any encryption mechanism, which is known as the sensitivity of the initial key parameters to the deciphered effect. To assess the key sensitivity of the presented mechanism, the ciphered Sailboat image is deciphered with tiny changes of initial values as shown in Fig. 7.

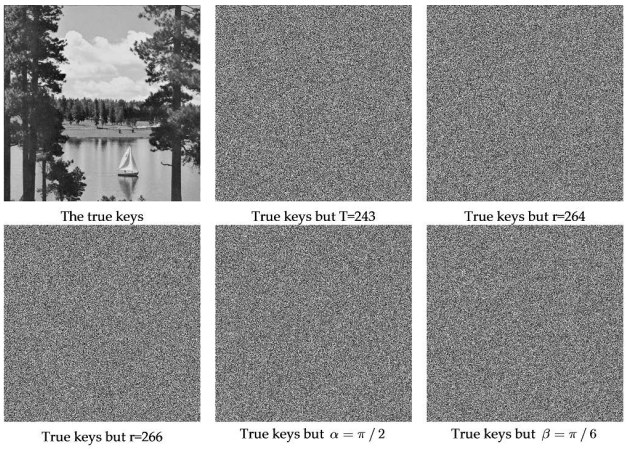


**FIGURE 7.** Decrypted image Sailboat with several keys.

### G. DISCUSSION

We have designed a new lightweight image encryption mechanism based on QWs for securing data transfers in IoT platforms. The presented solution utilises the capabilities of nonlinear dynamics of QWs to generate PRNG sequences and construct P-boxes. At first, the plain image is divided into blocks, and then each block is divided into two subblocks. Each subblock before recombination with each other is permutated and substituted with its own P-box and PRNG sequence that originates from the probability distribution of running QW. The ciphered blocks are combined together and then XORed with another PRNG sequence to construct the ciphered image. Several enclosed simulation and numerical analyses are conducted based on differential and statistical analyses, which affirm the effectiveness of the proposed cipher. The resulted cipher images have randomness properties, no useful data about the ciphered image can be obtained via analyzing the correlation of adjacent pixels. Moreover, the entropy value is close to the optimal value, NPCR test rate is greater than 99.61%, and there is high key sensitivity in the parameters of the keys with large keyspace to resist various cyberanalysis. In addition, to ensure the effectiveness of the presented mechanism, Table 5 provides a comparison with other related schemes which its construction is based on QWs.

**TABLE 5.** Comparison of average values of correlation coefficients, information entropy, and NPCR of the proposed approach with other related schemes which its construction is based on QWs.

| Algorrithm | Correlation | | | NPCR % | Entropy |
|---|---|---|---|---|---|
| | H | V | D | | |
| Proposed | -0.00063 | -0.00005 | 0.00057 | 99.618 | 7.9993 |
| Ref. [32] | 0.0002 | 0.00135 | 0.0006 | 99.614 | 7.9972 |
| Ref. [36] | -0.0067 | -0.0021 | -0.0027 | 99.58 | 7.9971 |
| Ref. [37] | -0.0022 | -0.0025 | -0.0035 | 99.619 | 7.9981 |
| Ref. [40] | -0.0023 | -0.0031 | -0.0091 | 99.598 | 7.9972 |

## VI. CONCLUSIONS

This work has introduced a new lightweight image encryption mechanism which is based on QW and which is destined for secure data transfers in IoT environments. The proposed solution utilises the probability distribution of running one-walker QW to construct P-boxes and to generate PRNG sequences for encrypting a plain image after dividing it into blocks. Perfomed simulations and statistical analysis confirmed that the suggested encryption scheme has high efficiency in terms of randomness tests,correlation coefficients, NPCR, information entropy, and histogram analysis. In addition to the formulation and application presented here, our proposal can be applied in digital computers as quantum-inspired quantum-walk protocols. Along the same lines, our approach can be utilized as quantum-inspired quantum-walk procedures for designing various encryption applications such as video, file, audio, etc.

## ACKNOWLEDGMENT

The authors would like to thank the family for their unconditional support.

## REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.
[2] H. Liao, Z. Zhou, X. Zhao, L. Zhang, S. Mumtaz, A. Jolfaei, S. H. Ahmed, and A. K. Bashir, "Learning-based context-aware resource allocation for edge computing-empowered industrial IoT," *IEEE Internet Things J.*, early access, Dec. 31, 2019, doi: 10.1109/JIOT.2019.2963371.
[3] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in Internet of Things and wearable devices," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 1, no. 2, pp. 99–109, Apr. 2015.
[4] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[5] J. Xiong, L. Chen, M. Z. A. Bhuiyan, C. Cao, M. Wang, E. Luo, and X. Liu, "A secure data deletion scheme for IoT devices through key derivation encryption and data analysis," *Future Gener. Comput. Syst.*, early access, Nov. 2, 2019, doi: 10.1016/j.future.2019.10.017.

[6] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the Internet of Things," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 12–18, Dec. 2018.

[7] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving fusion of IoT and big data for e-health," *Future Gener. Comput. Syst.*, vol. 86, pp. 1437–1455, Sep. 2018.

[8] Z. Zhou, X. Chen, Y. Zhang, and S. Mumtaz, "Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks," *IEEE Netw.*, vol. 34, no. 1, pp. 24–31, Jan. 2020.

[9] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri, and B. B. Gupta, "Efficient quantum information hiding for remote medical image sharing," *IEEE Access*, vol. 6, pp. 21075–21083, 2018.

[10] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy, and A. Ghoneim, "Secure quantum steganography protocol for fog cloud Internet of Things," *IEEE Access*, vol. 6, pp. 10332–10340, 2018.

[11] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. A. El-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Inf. Sci.*, vol. 515, pp. 191–217, Apr. 2020.

[12] A. K. Singh, B. Kumar, S. K. Singh, S. P. Ghrera, and A. Mohan, "Multiple watermarking technique for securing online social network contents using back propagation neural network," *Future Gener. Comput. Syst.*, vol. 86, pp. 926–939, Sep. 2018.

[13] N. N. Hurrah, S. A. Parah, N. A. Loan, J. A. Sheikh, M. Elhoseny, and K. Muhammad, "Dual watermarking framework for privacy protection and content authentication of multimedia," *Future Gener. Comput. Syst.*, vol. 94, pp. 654–673, May 2019.

[14] T. Tuncer, S. Dogan, R. Tadeusiewicz, and P. Pławiak, "Improved reference image encryption methods based on 2K correction in the integer wavelet domain," *Int. J. Appl. Math. Comput. Sci.*, vol. 29, no. 4, pp. 817–829, Dec. 2019.

[15] A. A. A. El-Latif, B. Abd-El-Atty, and M. Talha, "Robust encryption of quantum medical images," *IEEE Access*, vol. 6, pp. 1073–1081, 2018.

[16] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, Mar. 2015.

[17] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 127–133, Jan. 2017.

[18] L. Li, B. Abd-El-Atty, A. A. El-Latif, and A. Ghoneim, "Quantum color image encryption based on multiple discrete chaotic systems," in *Proc. Federated Conf. Comput. Sci. Inf. Syst.*, Sep. 2017, pp. 555–559.

[19] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new beta chaotic maps," *Opt. Lasers Eng.*, vol. 96, pp. 39–49, Sep. 2017.

[20] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," *Inf. Sci.*, vol. 396, pp. 97–113, Aug. 2017.

[21] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, pp. 225–237, Mar. 2017.

[22] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, Jan. 2017.

[23] D.-C. Lou and C.-H. Sung, "A steganographic scheme for secure communications based on the chaos and euler theorem," *IEEE Trans. Multimedia*, vol. 6, no. 3, pp. 501–509, Jun. 2004.

[24] C. Li, S. Li, and K.-T. Lo, "Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 2, pp. 837–843, 2011.

[25] C. H. Bennett and D. P. DiVincenzo, "Quantum information and computation," *Nature*, vol. 404, no. 6775, pp. 247–255, 2000.

[26] B. Abd-El-Atty, S. E. Venegas-Andraca, and A. A. A. El-Latif, "Quantum information protocols for cryptography," in *Quantum Computing: An Environment for Intelligent Large Scale Real Application*. Cham, Switzerland: Springer, 2018, pp. 3–23.

[27] R. Arul, G. Raja, A. O. Almagrabi, M. S. Alkatheiri, S. H. Chauhdary, and A. K. Bashir, "A quantum-safe key hierarchy and dynamic security association for LTE/SAE in 5G scenario," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 681–690, Jan. 2020.

[28] S. E. Venegas-Andraca, "Quantum walks: A comprehensive review," *Quantum Inf. Process.*, vol. 11, no. 5, pp. 1015–1106, Oct. 2012.

[29] A. M. Childs, "Universal computation by quantum walk," *Phys. Rev. Lett.*, vol. 102, no. 18, May 2009, Art. no. 180501.

[30] A. M. Childs, D. Gosset, and Z. Webb, "Universal computation by multiparticle quantum walk," *Science*, vol. 339, no. 6121, pp. 791–794, Feb. 2013.

[31] A. A. A. El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, and W. Mazurczyk, "Efficient quantum-based security protocols for information sharing and data protection in 5G networks," *Future Gener. Comput. Syst.*, vol. 100, pp. 893–906, Nov. 2019.

[32] A. A. A. El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, "Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," *Sci. Rep.*, vol. 10, no. 1, pp. 1–16, Dec. 2020.

[33] Y.-G. Yang, Q.-X. Pan, S.-J. Sun, and P. Xu, "Novel image encryption based on quantum walks," *Sci. Rep.*, vol. 5, no. 1, Jul. 2015, Art. no. 7784.

[34] Y.-G. Yang, P. Xu, R. Yang, Y.-H. Zhou, and W.-M. Shi, "Quantum hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption," *Sci. Rep.*, vol. 6, no. 1, Apr. 2016, Art. no. 19788.

[35] A. A. A. El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Opt. Laser Technol.*, vol. 116, pp. 92–102, Aug. 2019.

[36] B. Abd-El-Atty, A. A. A. El-Latif, and S. E. Venegas-Andraca, "An encryption protocol for NEQR images based on one-particle quantum walks on a circle," *Quantum Inf. Process.*, vol. 18, no. 9, p. 272, Sep. 2019.

[37] A. A. A. El-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, "Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things," *Opt. Laser Technol.*, vol. 124, Apr. 2020, Art. no. 105942.

[38] A. A. A. El-Latif, B. Abd-El-Atty, S. Elseuofi, H. S. Khalifa, A. S. Alghamdi, K. Polat, and M. Amin, "Secret images transfer in cloud system based on investigating quantum walks in steganography approaches," *Phys. A, Stat. Mech. Appl.*, vol. 541, Mar. 2020, Art. no. 123687.

[39] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G Internet of Things scenario," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 1, pp. 118–131, Mar. 2020.

[40] A. A. A. El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption," *Phys. A, Stat. Mech. Appl.*, vol. 547, Jun. 2020, Art. no. 123869.

[41] D. Li, Y.-G. Yang, J.-L. Bi, J.-B. Yuan, and J. Xu, "Controlled alternate quantum walks based quantum hash function," *Sci. Rep.*, vol. 8, no. 1, pp. 1–7, Dec. 2018.

[42] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[43] M. M. Rathore, A. Ahmad, A. Paul, and S. Rho, "Urban planning and building smart cities based on the Internet of Things using big data analytics," *Comput. Netw.*, vol. 101, pp. 63–80, Jun. 2016.

[44] A. K. Bashir, R. Arul, S. Basheer, G. Raja, R. Jayaraman, and N. M. F. Qureshi, "An optimal multitier resource allocation of cloud RAN in 5G using machine learning," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 8, Aug. 2019, Art. no. e3627.

[45] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[46] S. Pirbhulal, O. W. Samuel, W. Wu, A. K. Sangaiah, and G. Li, "A joint resource-aware and medical data security framework for wearable healthcare systems," *Future Gener. Comput. Syst.*, vol. 95, pp. 382–391, Jun. 2019.

[47] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[48] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A review," in *Proc. Int. Conf. Comput. Sci. Electron. Eng.*, vol. 3, 2012, pp. 648–651.

[49] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for Internet of Things," in *Proc. Int. Symp. Next-Gener. Electron. (ISNE)*, May 2014, pp. 1–2.

**AHMED A. ABD EL-LATIF** (Member, IEEE) received the B.Sc. degree (Hons.) in mathematics and computer science and the M.Sc. degree in computer science from Menoufia University, Egypt, in 2005 and 2010, respectively, and the Ph.D. degree in computer science and technology from the Harbin Institute of Technology (H.I.T), Harbin, China, in 2013. He is currently an Associate Professor of computer science with Menoufia University, Egypt and School of Information Technology and Computer Science, Nile University, Egypt. He has authored or coauthored more than 100 articles, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, and book chapters. He received many awards, the State Encouragement Award in Engineering Sciences 2016, the Arab Republic of Egypt, the Best Ph.D. Student Award from the Harbin Institute of Technology, China 2013, and the Young Scientific Award, Menoufia University, Egypt 2014. He is a fellow at the Academy of Scientific Research and Technology, Egypt. His areas of interests are multimedia content encryption, secure wireless communication, IoT, applied cryptanalysis, perceptual cryptography, secret media sharing, information hiding, biometrics, forensic analysis in digital images, and quantum information processing. Dr. Abd El-Latif has many collaborative scientific activities with international teams in different research projects. Furthermore, he has been reviewing article for 85+ International Journals including the *IEEE Communications Magazine*, the IEEE Internet of Things journal, *Information Sciences*, the IEEE Transactions on Network and Service Management, the IEEE Transactions on Services Computing, *Scientific Reports*, *Nature*, the *Journal of Network and Computer Applications*, *Signal Processing*, *Cryptologia*, *Journal of Network and Systems Management, Visual Communication and Image Representation*, *Neurocomputing*, *Future Generation Computer Systems*, etc. He is an Associate Editor of the *Journal of Cyber Security and Mobility*.

**BASSEM ABD-EL-ATTY** received the B.S. degree in physics and computer science, the M.Sc. degree in computer science, and the Ph.D. degree in computer science from Menoufia University, Egypt, in 2010, 2017, and 2020, respectively. He has authored or coauthored more than 20 articles, including refereed the IEEE/Springer/Elsevier journals, conference papers, and book chapters. He is a Reviewer in a set of reputable journals in Elsevier and Springer. His research interests include quantum information processing and image processing.

**SALVADOR E. VENEGAS-ANDRACA** received the M.Sc. degree in artificial intelligence and the D.Phil. degree in physics and the from the University of Oxford, in 2002 and 2006, respectively, and the M.B.A. (Hons.) and B.Sc. (Hons.) degrees in digital electronics and computer science from the Tecnológico de Monterrey. He is currently a Professor of computer science and the Head of the Quantum Information Processing Group, Tecnológico de Monterrey, Mexico. He is also a Leading Scientist in the field of quantum walks and cofounder of the field quantum image processing. His research interests include quantum algorithms as well as the algorithmic analysis of NP-hard/NP-complete problems. He has published more than 50 scientific articles, he has authored *Quantum Walks for Computer Scientists*, in 2008, the first book ever written on the scientific field of quantum walks, and coauthored *Quantum Image Processing*, in 2020, the first book totally focused on processing visual information using quantum systems. He has lectured in eleven countries across three continents and has been a Visiting Professor at Harvard University, the National Autonomous University of Mexico, del Valle University, Colombia, Bahia Blanca University, Argentina, and Yucatan University, Mexico. He is a fellow of the Mexican Academy of Sciences and a Senior Member of the Association for Computing Machinery.

**HAITHAM ELWAHSH** received the B.Sc. degree from the Faculty of Science-Qena, South Valley University, in 2004, the M.Sc. degree in computer science from Menoufia University, in 2012, and the Ph.D. degree of science in mathematics and computer science from Port Said University, Egypt, in 2019. He is currently an Assistant Professor with Computer Science Department, Faculty of Computers and Information, Kafrelsheikh University, Kafrelsheikh, Egypt. His research interests include network security and image processing.

**MD. JALIL PIRAN** (Member, IEEE) received the Ph.D. degree in electronics and radio engineering from Kyung Hee University, South Korea, in 2016. He is currently working as a Postdoctoral Research Fellow in the field of resource management and quality of experience in 5G-cellular networks, and the Internet of Things with the Networking Laboratory, Kyung Hee University. He is also a Professor with the Department of Computer Science and Engineering, Sejong University, Seoul, South Korea. He has published substantial number of technical articles in well-known international journals and conferences in research fields of: resource allocation and management in; 5G mobile and wireless communication, HetNet, the Internet of Things (IoT), multimedia communication, streaming, adaptation, and QoE, cognitive radio networks, wireless sensor networks, machine learning, fuzzy logic, and neural networks. He was a recipient of IAAM Scientist Medal of the year 2017 for Notable and Outstanding Research in the field of New Age Technology and Innovation, in Stockholm, Sweden. Moreover, He has been recognized as the Outstanding Emerging Researcher by the Iranian Ministry of Science, Technology, and Research, in 2017. In addition, his Ph.D. dissertation has been selected as the Dissertation of the Year 2016 by the Iranian Academic Center for Education, Culture, and Research in the field of electrical and communications engineering. In the worldwide communities, he has been an Active Delegate from South Korea in the Moving Picture Experts Group (MPEG), since 2013, and an Active Member of the International Association of Advanced Materials (IAAM), since 2017.

**ALI KASHIF BASHIR** is currently with the School of Computing and Mathematics, Manchester Metropolitan University, U.K. He is also attached to the School of Electrical Engineering and Computer Science, National University of Science and Technology, Islamabad (NUST) as an Adjunct Professor. He is a Distinguished Speaker of ACM. His past assignments include an Associate Professor of Information and Communication Technologies, Faculty of Science and Technology, University of the Faroe Islands, Denmark; Osaka University, Japan (71 in QS Ranking 2020); Nara National College of Technology, Japan; the National Fusion Research Institute, South Korea; Southern Power Company Ltd., South Korea, and the Seoul Metropolitan Government, South Korea. He has advised several startups in the field of STEM-based education, robotics, and smart homes. A few of these are RNS Solutions, Edvon, UHom, and Bandz Network.

**OH-YOUNG SONG** received the B.S., M.S., and Ph.D. degrees from the School of Electrical Engineering and Computer Science, Seoul National University, South Korea, in 1998, 2000, and 2004, respectively. He was a Postdoctoral Fellow with the School of Electrical Engineering and Computer Science, Seoul National University, South Korea, from 2004 to 2006. He is currently an Associate Professor with the Department of Software, Sejong University, South Korea. His research interests include computer graphics, simulation, and machine learning. Especially, he has contributed in the areas of physics-based animation, human motion, numerical algorithms, VR/AR, medical image analysis, and deep learning.

**WOJCIECH MAZURCZYK** received the B.Sc., M.Sc., Ph.D. (Hons.), and D.Sc. (habilitation) degrees in telecommunications from the Warsaw University of Technology (WUT), Warsaw, Poland, in 2003, 2004, 2009, and 2014, respectively. He is currently an Associate Professor with the Institute of Telecommunications, WUT, where he is the Head of the Bio-Inspired Security Research Group. He is also a Researcher with the Parallelism and VLSI Group, Faculty of Mathematics and Computer Science, FernUniversitaet, Germany. His research interests include bioinspired cybersecurity and networking, information hiding, and network security. He is involved in the technical program committee of many international conferences and also serves as a reviewer for major international magazines and journals. From 2016, he was the Editor-in-Chief of an open access *Journal of Cyber Security and Mobility*, and since 2018, he has been serving as an Associate Editor of the IEEE Transactions on Information Forensics and Security and as *Mobile Communications and Networks Series* an Editor for the IEEE Communications Magazine.